# 实验一 接管裸机的控制权

实验人：张海涛 张晗宇 张浩然 张镓伟

学号：15352405 15352406 15352407 15352408

院系：数据科学与计算机学院

专业、年级： 15级移动信息工程

指导老师：凌应标

## 实验题目

## 接管裸机的控制权

## 二、实验目的

## 搭建和运用实验环境、接管裸机的控制权

## 三、实验要求

## 1.虚拟机安装，生成一个基本配置的虚拟机 PC和多个 1.44MB容量的虚拟软盘，将其中一个虚拟软盘用 DOS格式化为 DOS引导盘，用 WinHex工具将其中一个虚拟软盘的首扇区填满你的个人信息。

2。设计 IBM\_PC的一个引导扇区程序，程序功能是：用字符‘A’从屏幕左边某行位置 45度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后产生反射，改变方向运动，如此类推，不断运动；在此基础上，增加你的个性扩展，如同时控制两个运动的轨迹，或炫酷动态变色，个性画面，如此等等，自由不限。还要在屏幕某个区域特别的方式显示你的学号姓名等个人信息。将这个程序的机器码放进放进第三张虚拟软盘的首扇区，并用此软盘引导你的 XXXPC，直到成功。

## 四、实验方案

1.虚拟机配置方法

无操作系统，10M硬盘，4MB内存，启动时连接软盘

2.软件工具和作用

Notepad++:用于生成.汇编语言文件

Nasm：用于编译.asm类型的汇编语言文件，生成bin文件

Vmware Workstation 12Player: 用于创建虚拟机，模拟裸机环境

Bochs： 用于创建空的虚拟软盘

WinHex: 用于编辑img文件的扇区数据

1. 方案思想
2. 实验题目一

①使用Bochs内置的Disk image creation tool创建一个符合要求的空盘。

②使用虚拟机运行空盘，使用dos指令将软盘格式化成dos引导盘。

③使用汇编语言，利用times指令，将前510个字节填满个人信息，最后两个字节是0aa55h，编译生成得到软盘镜像文件，使用Winhex软件检查确认符合题目要求。

1. 实验题目二

①字符的动态显示

将字符的运动状态保存下来，并与显示界面边界比较更新下一个运动状态（包括运动方向、字符的位置、字符的颜色、字符的内容），利用延时和循环显示出字符的运动轨迹。

②个人信息显示

将两个字符串利用循环显示在界面的中间位置。

1. 相关原理
2. 在屏幕上显示文字

显示器

将那些内容以视觉可见的方式呈现在屏幕上。

显示卡

为显示器提供内容，并控制显示器的显示模式和状态

图形方式：最小可控制单位为像素，VGA：640X400

文本方式：最小可控制单位为字符，VGA：25X80

显示卡内存：存放像素或文字及相关属性



1. 字符显示原理

字符发生器和控制电路

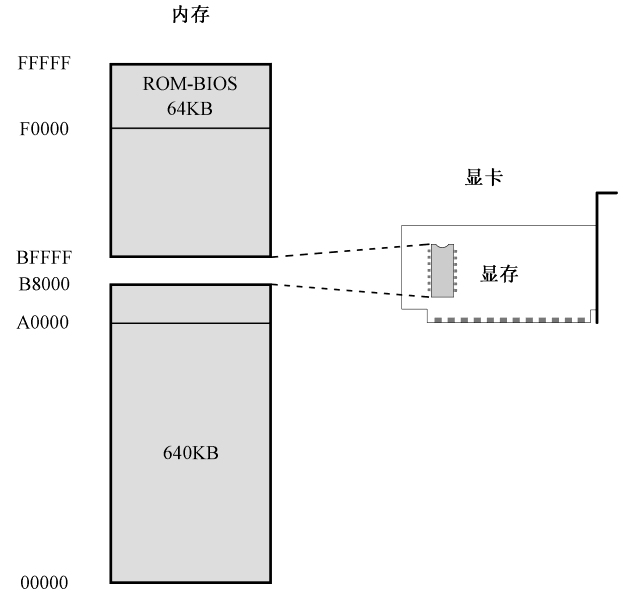
用代码来控制屏幕上的像素，使它们或明或暗以构成字符的轮廓



（3）字符方式显存地址空间

8086可访问的内在1MB

地址空间B8000~BFFFF，共32KB



1. 初始化段寄存器

访问显存使用逻辑地址

采用“段地址：偏移地址”的形式

显存段地址B800

初始化段寄存器

规定：

不能将立即数直接传送到段寄存器

防止误操作

（5）显存与屏幕上字符的对应



（6）屏幕上字符的显示属性

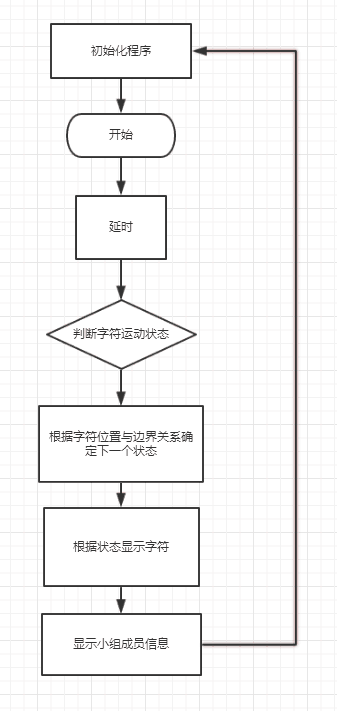


1. 显示字符

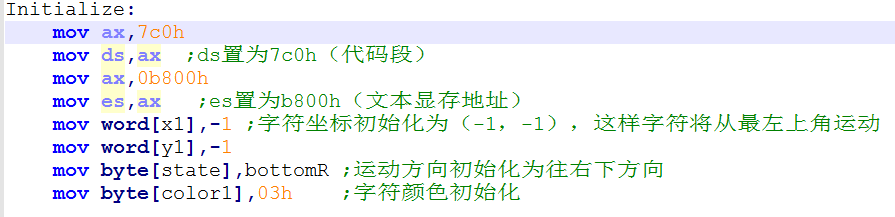
把字符的ASC码和属性编码送到对应的显存中

1. X86汇编语言语法

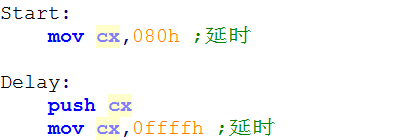
5.程序流程



1. 程序关键模块
2. 初始化过程



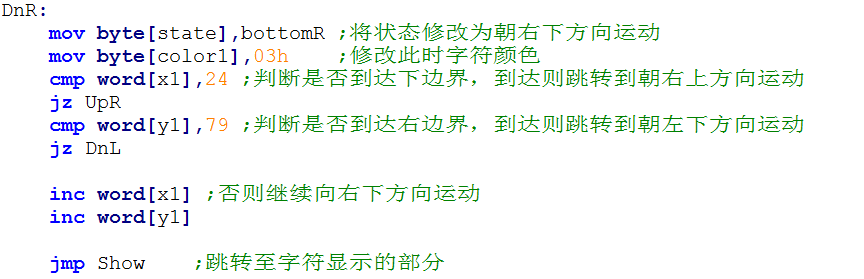
1. 开始程序，进行延时



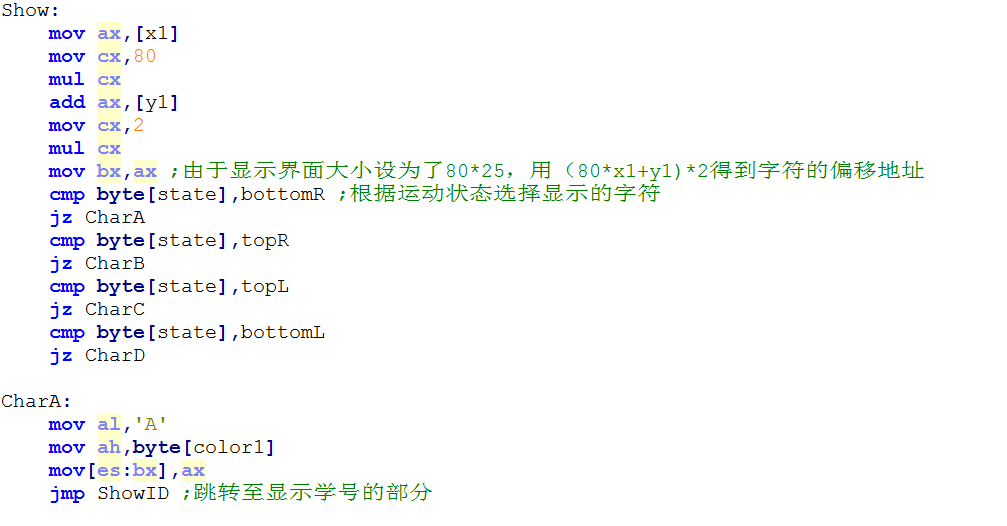
1. 判断当前状态



1. 判断下一状态，修改相关信息（以现在是朝右下方向为例）



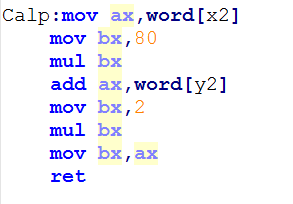
（5）显示字符（以现在是朝右下方向为例）



1. 显示两行字符串（个人信息）



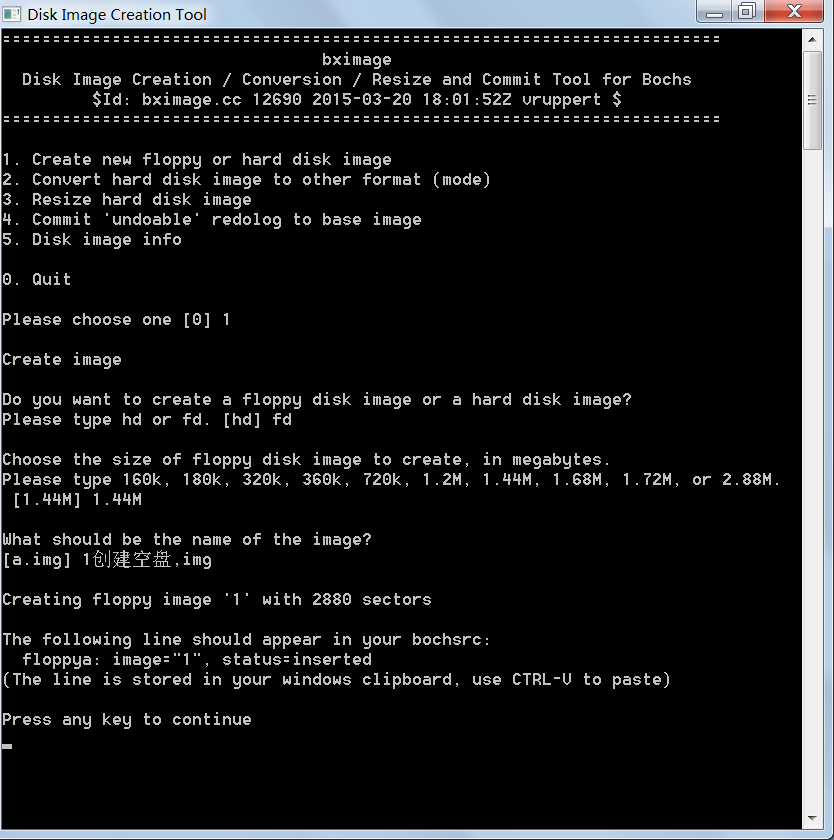
1. 调用函数计算偏移地址



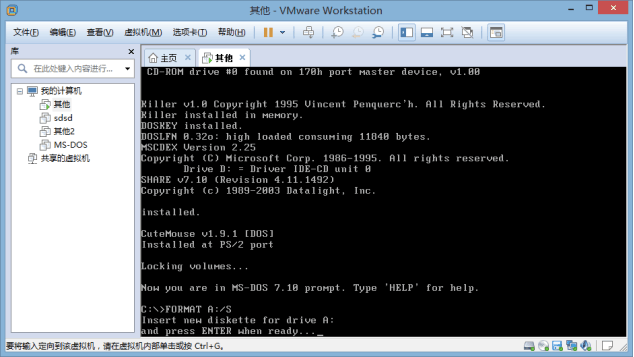
## 实验过程

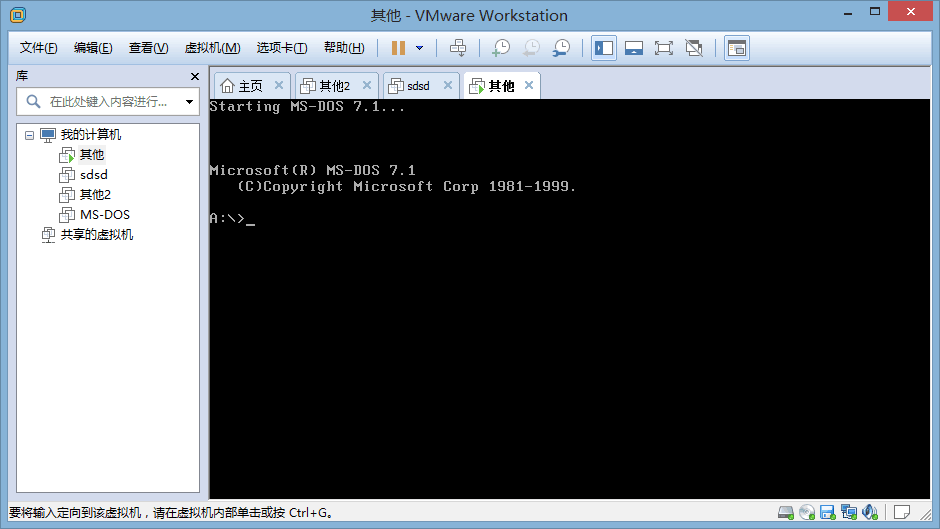
1. 实验题目一

①创建空盘

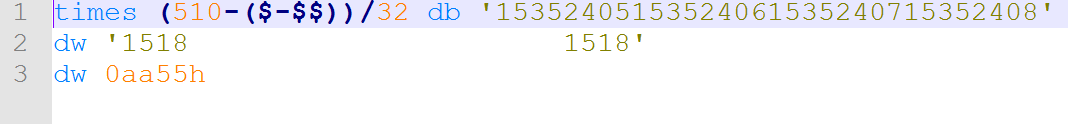


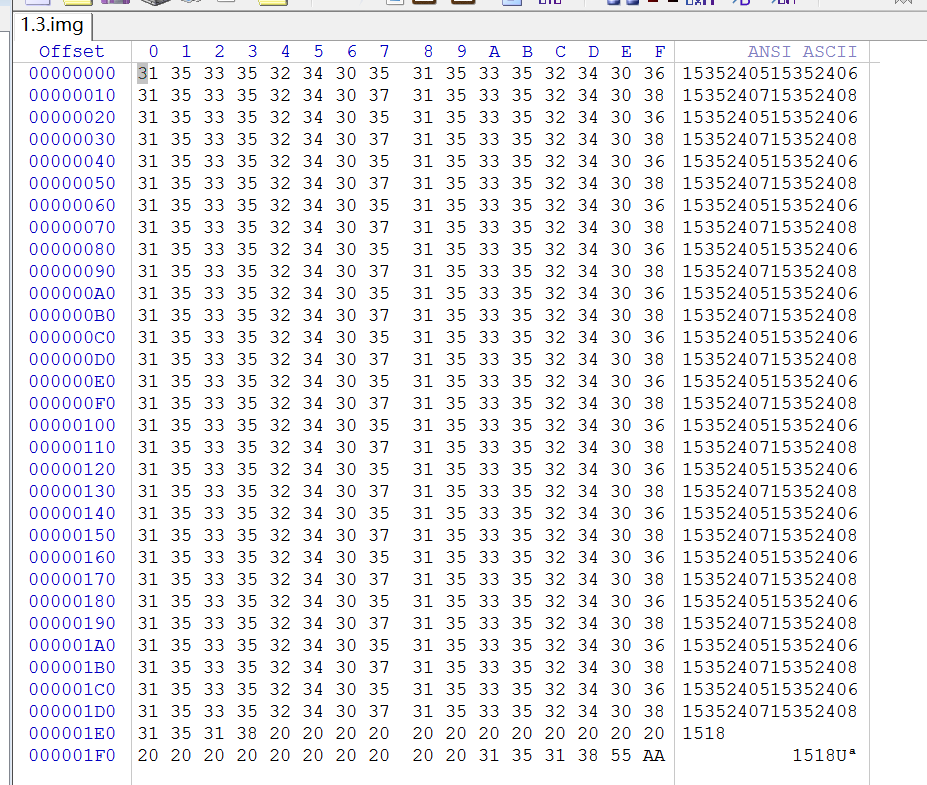
②使用DOS格式化空盘为DOS引导盘





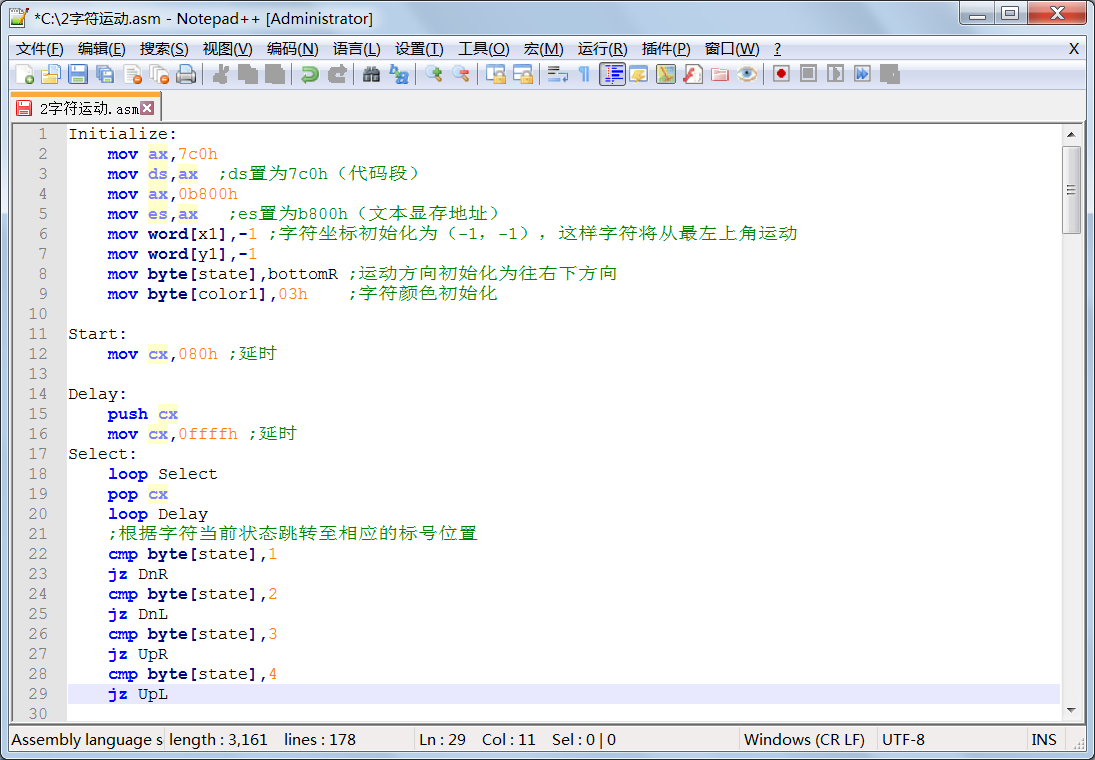
③将首扇区填满个人信息





1. 实验题目二

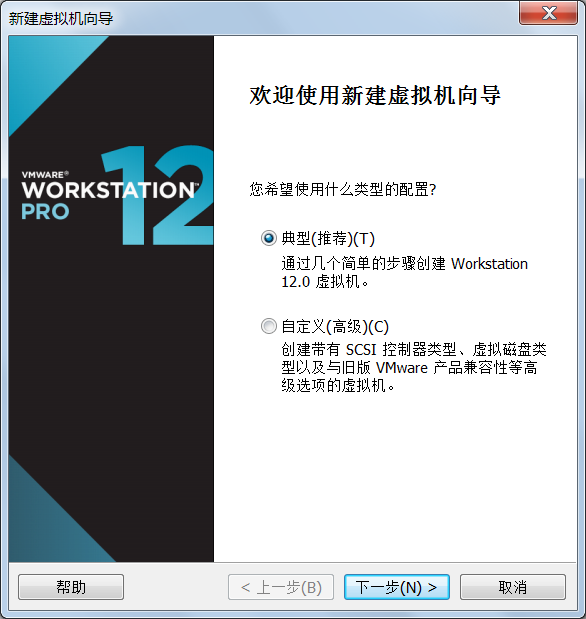
步骤一：编写asm代码



步骤二：使用nasm软件编译成软盘镜像文件

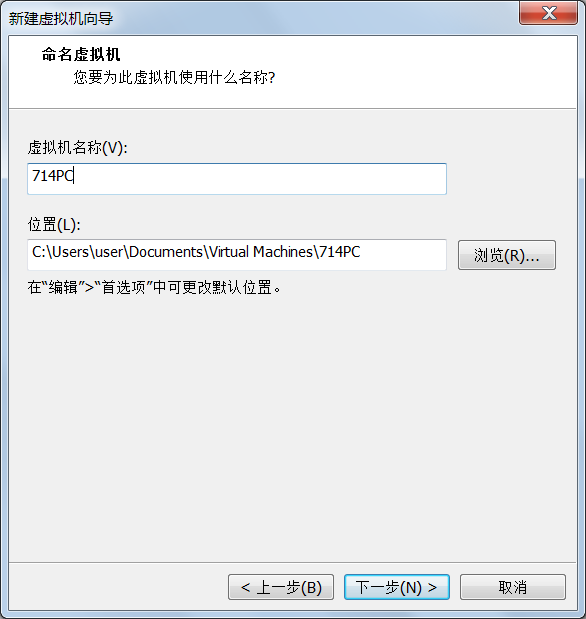


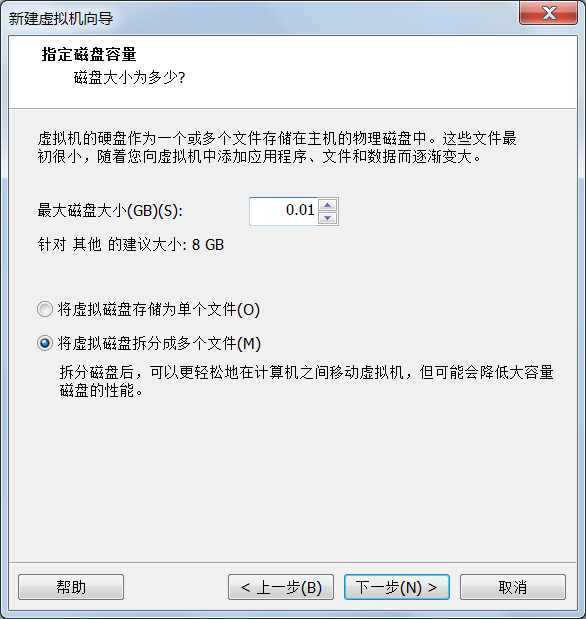
步骤三：在虚拟机上运行

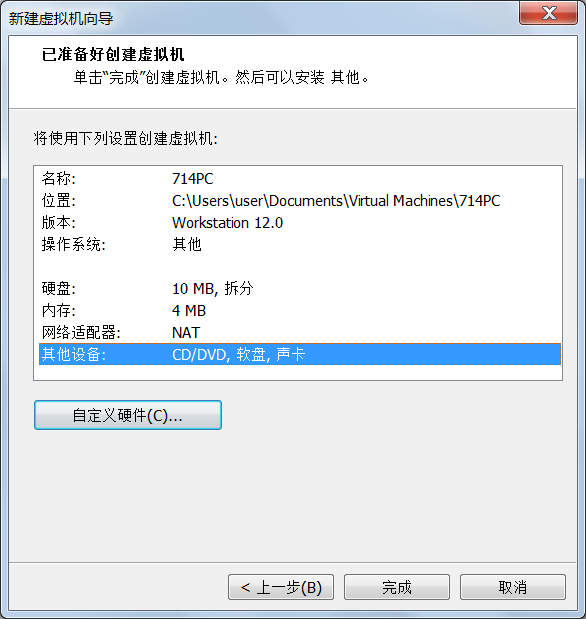


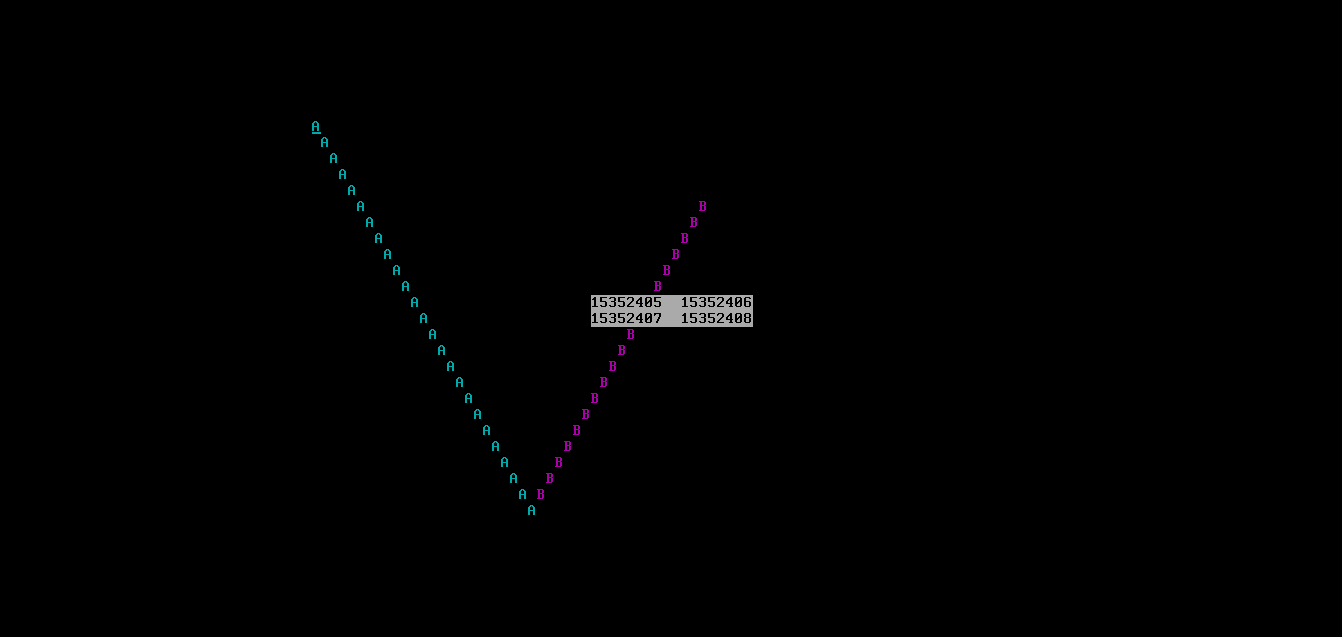


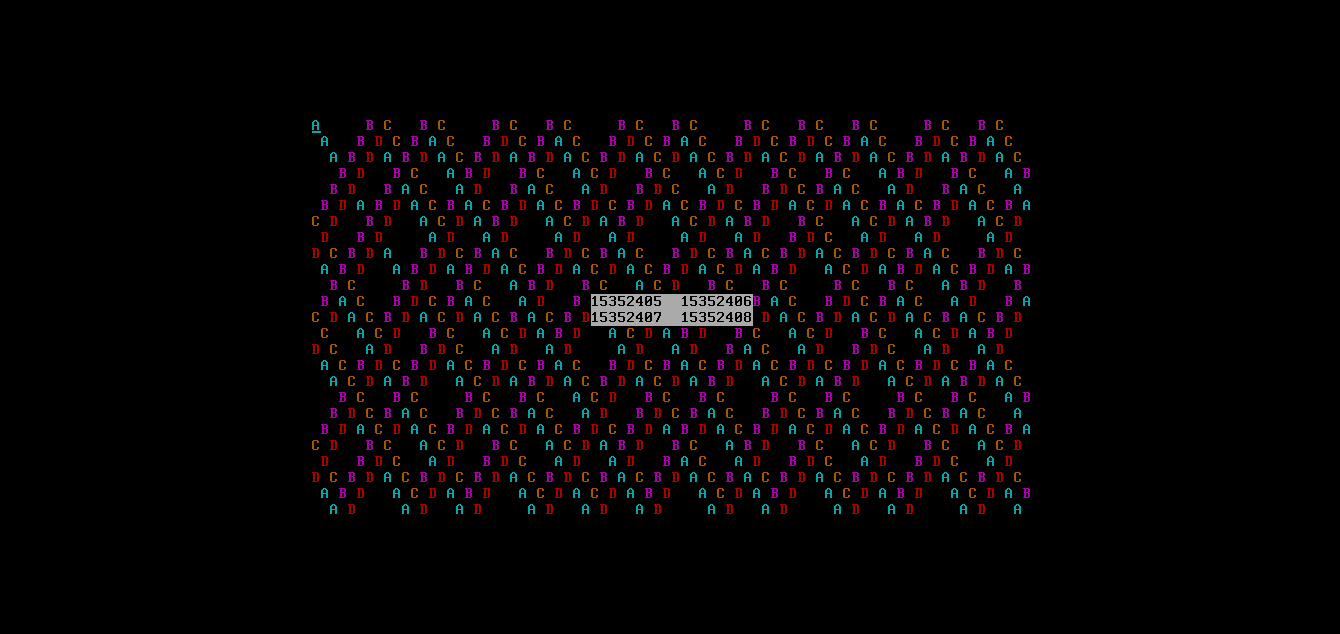












1. 遇到关键问题

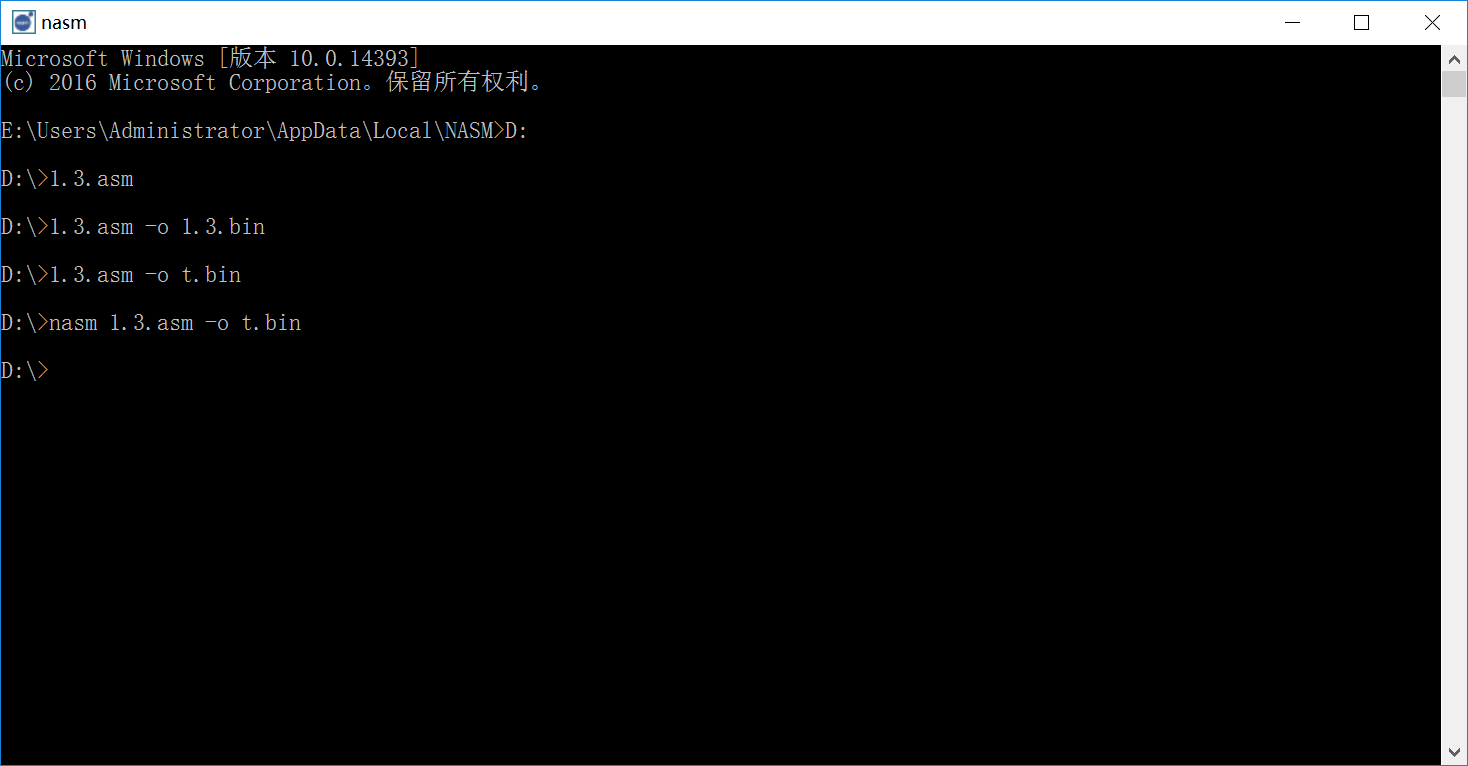
四行字符串无法完整显示，研究了很久才发现是超过了512k，最后改用两行显示，删掉两个循环。

## 五、实验总结

（1）张海涛实验心得：

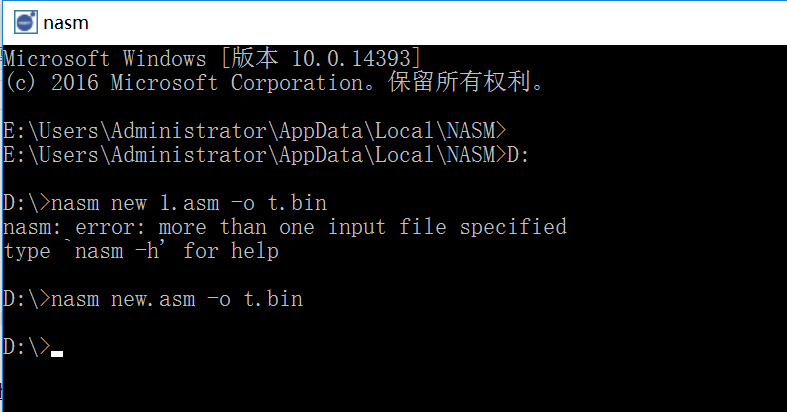
在做实验三（填充个人信息）时，我参考了老师给的资料，可以使用三行代码实现。可是代码是什么意思呢？通过查询知道：times XXX db 0 ; 这个表示填充XXX个字节的0，所以，times 510-($-$$) db 0，表示填充 510-($-$$) 这么多个字节的0，这里面的$表示当前指令的地址，$$表示程序的起始地址(也就是最开始的7c00)，所以$-$$就等于本条指令之前的所有字节数。510-($-$$)的效果就是，填充了这些0之后，从程序开始到最后一个0，一共是510个字节。再加上最后的dw两个字节(0xaa55是结束标志)，整段程序的大小就是512个字节，刚好占满一个扇区。

在将汇编文件生成可执行.bin文件的时候，认识到了nasm生成文件的指令格式。



nasm -f <format> <filename> [-o <output>]

打开方式 输入文件（格式） -o 输入文件（格式）

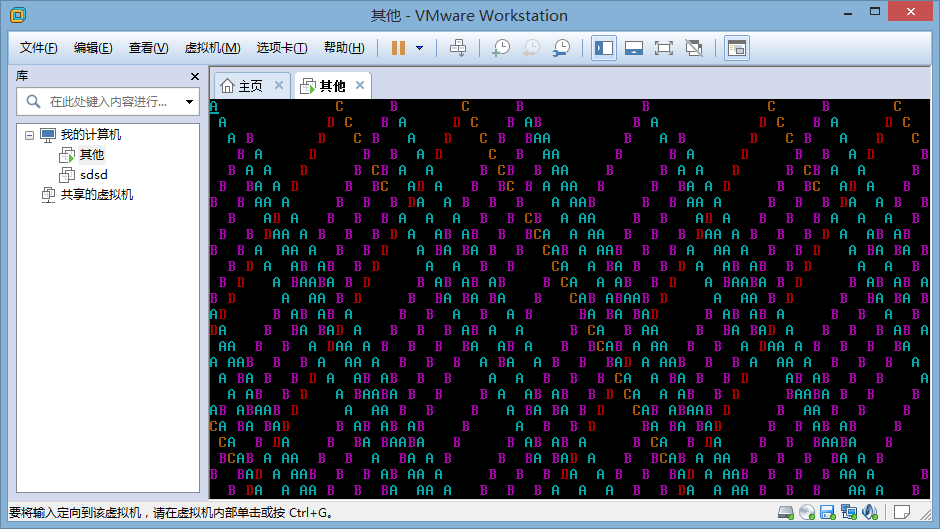


在后面的生成过程中，遇到了报错。我尝试几次之后终于发现了问题所在：文件名不能包含空格，否则系统就会认为是两个部分，然后报错。

初次做操作系统的实验：需要用到的软件不少，但是了解到他们各自的用途之后，我对操作系统的生成有了初步认识，面对一台裸机（vmware生成），需要使用软盘作为引导（操作系统最初的作用），只有通过引导，我们才能获取到计算机的控制权，才能运行自己的程序。软盘的制作过程也加深了我对程序概念的认识：从高级语言编译得到汇编语言，然后链接生成可执行的文件，电脑才能执行。

1. 张晗宇实验心得：

一开始学习做操作系统，在汇编语言没有学习完的情况下，一开始毫无头绪，不懂dos引导盘如何制作，也不能理解样例代码stoneM的代码意思，再加上stone无法转换为bin文件，导致一直没有进度。只能先看X86汇编书籍学习，百度代码，查找用法与意思。然后看着满分项目的代码照猫画虎，一条条代码去理解，过程艰难而漫长，在实现A的滚动和显示学号的过程中，出现了不少问题，我们先试图单独使A动态变化，为了让A有所不同，我们设置使得他遇到不同的墙壁变为不同的字母与颜色，导致加了不少的代码，使得最后超过512字节，还有由于一个小失误将一个y1写成了y2而导致字母A的滚动方式匪夷所思



再之后由于loop太多了导致显示学号出现了问题。我们一开始是显示4行，每个学号一行，这样就无形多了许多loop，但是我们并不知道是超了512kb的问题，一直检查，一直找不到原因，被迫一个一个注释掉再消掉注释观察现象，可能每个人都试了十几次才发现问题所在，最后通过将4个人的学号化为两行，减少loop，使得bin文件大小小于512字节才解决。最后不懂如何创建引导盘，从网上下过MS—DOS也没看出什么，满分项目的描述也是十分的模糊，最后我们通过不断尝试和搜索，发现只要在创建的空盘里输入指令format A:/S 即可创建引导盘。

（3）张浩然实验心得：

这次实验给我的收获非常大。在实验要求刚布置下来时，我只会老师在上课时演示的在屏幕上显示‘@’，同时代码也有很多地方不懂意思。在自己开始做实验时，我通过学习群里X86教材、在网上搜索相关资料、阅读给出的参考代码，对X86汇编语言有了初步的认识，对其中的一些语法规则和习惯用法、和背后的结构的理解进一步加深了。

在实验过程中，也遇到了很多的问题和障碍。第一个实验内容中，要求使用DOS格式化将一个空盘格式化为引导盘，在网上查询了dos的格式化指令后我百思不得其解，使用dos感觉只能将一个实际存在的硬盘或者软盘格式化，我该如何在将虚拟软盘在dos中格式化？后来同组成员在尝试后给了我答案——使用虚拟机软件运行这个虚拟机，然后在虚拟机中打入格式化的指令。我豁然开朗发现了自己之前思考问题的角度有些死板，没有将通用的解决方法灵活运用到具体情况之中。

第二个实验遇到的第一个问题是字符没有在运动，在检查过代码之后发现少了一个jmp，导致程序不能进行下去。第二个问题是字符开始运动后，朝右下方向运动撞到右边界时会穿过右边界，从左边界里出来。虽然我们花了不少时间研究为什么出现这样的错误，但最后发现是我把坐标y1写成了y2，当然也就不会按照规则运动了。这两个都可以说是写代码时粗心犯的错误，需要注意。

我们遇到了一个很大的障碍就是不能用四行完整地显示四个组员的学号，只能显示一两行，甚至在进行一些尝试后只能显示背景色。一开始我以为是哪一段代码写的有错误，导致无法正常显示字符串，但进行了多处的修改和调试之后依旧不能达到预计的效果。最后组员通过不停地注释掉一段代码来检查到哪里是没有问题，发现可能是超过512字节了，看了下文件属性，的确是超了。为了解决超字节的问题，我们最后使用了两行来显示四个人的学号，这样就减少了两个循环，的确也不超过512字节，达到了预计的效果了。不过在这个错误过程中，我也将字符串的显示进行了优化，原来的代码在模仿课本和参考代码时有一些多余的地方以及和我需求不同的地方，在研究后进行了优化。

在实验过程中让我觉得以后需要加强注意的就是不断练习自己写汇编语言的能力。虽然基本都能看懂汇编语言了，但自己还不能完全独立地写出来，需要不断地查资料，参考书本和别人的代码，代码也一定还有可以优化算法，精简代码内容的地方。这些还需要对汇编语言使用的积累。

（4）张镓伟实验心得：

操作系统的第一次实验，写引导程序，虽然这个是最简单的入门实验，但对我来说却是一次很大的挑战。最大的原因就是此前从来没有学过x86架构的汇编语言，计算机组成原理课学习的是MIPS架构的汇编，不能应用在此。所以我能半路出家，看文档《x86汇编语言-从实模式到保护模式》和百度各种指令，寄存器的意义等去快速学习。此后去钻研老师给的例程，在这里我又知道了写引导程序要知道一些特殊的地址，比如开始执行程序的起始地址是7c0h，文本窗口显存起始地址是0b800h。基本弄懂了一些语法之后，我们开始照猫画虎去写。这里主要遇到了两个问题。1.是由于打错表示纵坐标的变量而导致字的弹射出现了“穿墙”的情况。这里我们检查了很久才发现，所以写代码的时候一定要细心。2.是我们想用4行分别显示4个组员的学号却发现编译出来的bin文件大小已经超过了512k，后来我灵机一动，把两个学号当成一个字符串显示在一行，这样我们就可以减少显示第三行和第四行的代码。最终这样做之后果然把文件大小控制在了512k之内。这次实验我觉得还是学到了很多东西，希望后面的实验可以更加顺利。